
Ataques DDoS: Detecção, Prevenção e Mitigação
Uma Jornada pela Segurança Cibernética
IX FÓRUM
FORTALEZA
OPENIX

O Ambiente Atual da Internet

A verdadeira questão é:

"O que eu farei quando os ataques começarem?"

Quem sou eu?

- Trabalho com **ISPs** desde **1997**
- Estudo sobre **firewalls** desde 2000
- Fundador da **OpenX** em 2001
- Primeiros contatos com **DDoS** em 2009 (hosting)
- Estudioso de ataques **DDoS** desde 2014, inicio da operação de **Link IP** da **OpenX**

OPENX

Breves avisos

- YouTube.com/**openx**
- **Instagram:** @openxbr e @renatoornelas

OPENX

O Uso da Internet no Dia a Dia

- A **Internet** é mais importante do que nunca, principalmente desde o inicio da pandemia, evento que impulsionou a **digitalização** das nossas vidas.
- **Estudo, trabalho, compras, diversão**: tudo é feito atrás das telas
- Além disso o trafego entre equipamentos aumentou com tendencia de explodir **ainda mais** devido a IA e Realidade Virtual/aumentada
- Não basta não ficar fora, tudo tem que ser **rápido** e **sem engasgos** na conexão

OPENX

A ameaça: Ataques DDoS

- Um ataque de negação de serviço distribuído (DDoS) é uma forma de **ataque não intrusivo**, feito para derrubar um site, aplicação ou rede com tráfego forjado/falso ou refletido.
- Contra um alvo vulnerável é possível que até mesmo um volume relativamente pequeno de tráfego seja suficiente para **derrubar o alvo**.
- Um ataque DDoS envolve **múltiplas origens**, normalmente uma Botnet, **impedindo** a identificação do responsável pelo tráfego malicioso.

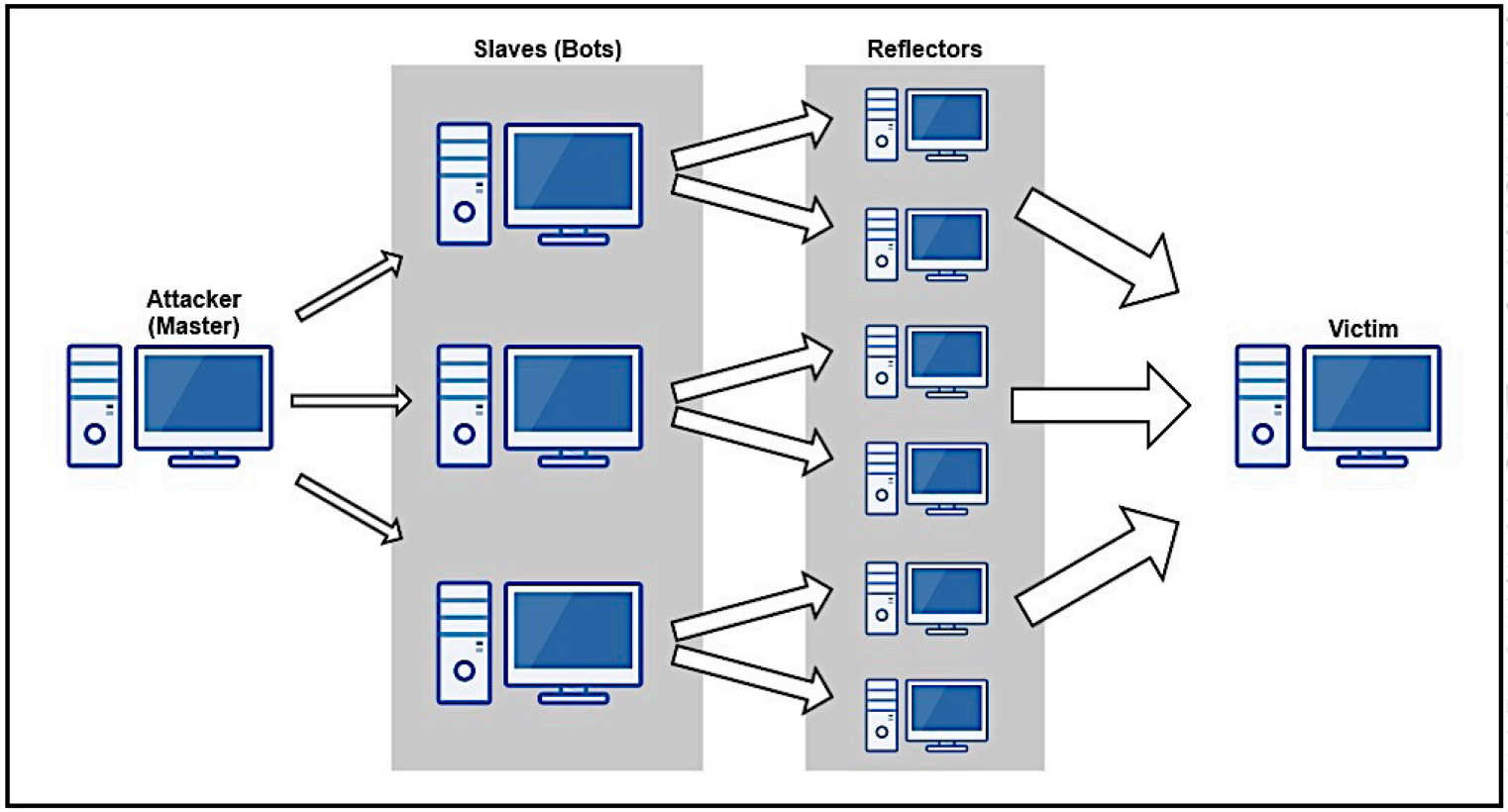
OPENX

Tipos de Ataque DDoS

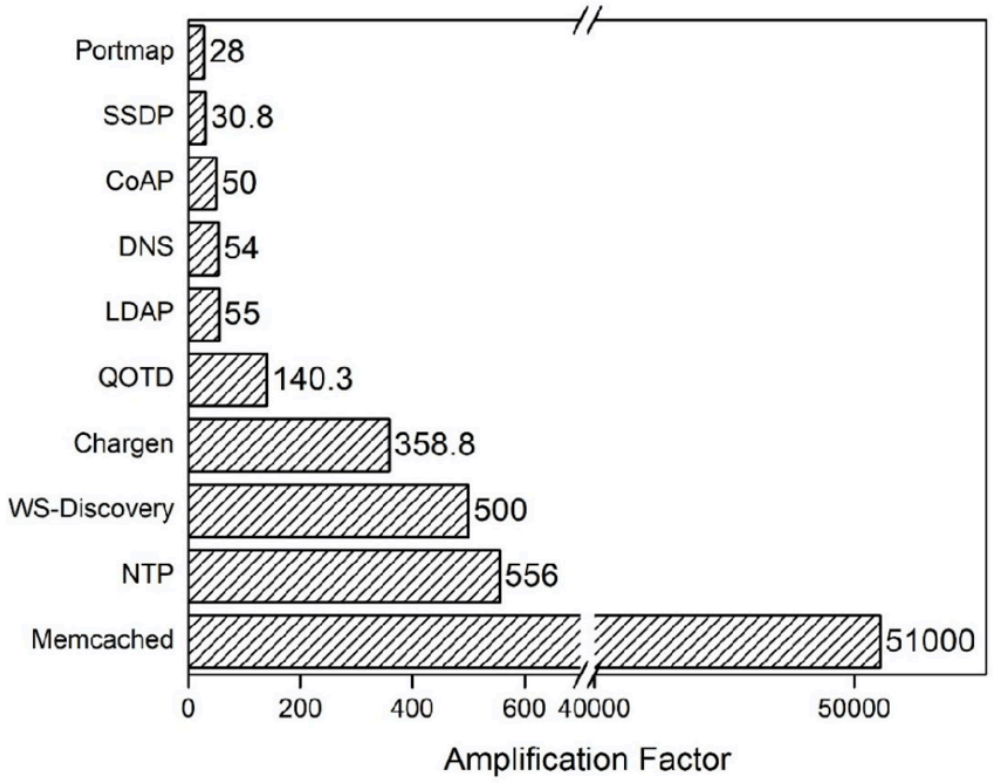
- **Volumétrico**: Muita banda ou muitos pacotes por segundo
- **Baseado em protocolos**: explora alguma falha de um protocolo
- **Aplicação**: Explora alguma falha de uma aplicação
- **Amplificação**: Explora a resposta de algum protocolo
- **Carpet Bomb**
- **Hit&Run**

OPENX

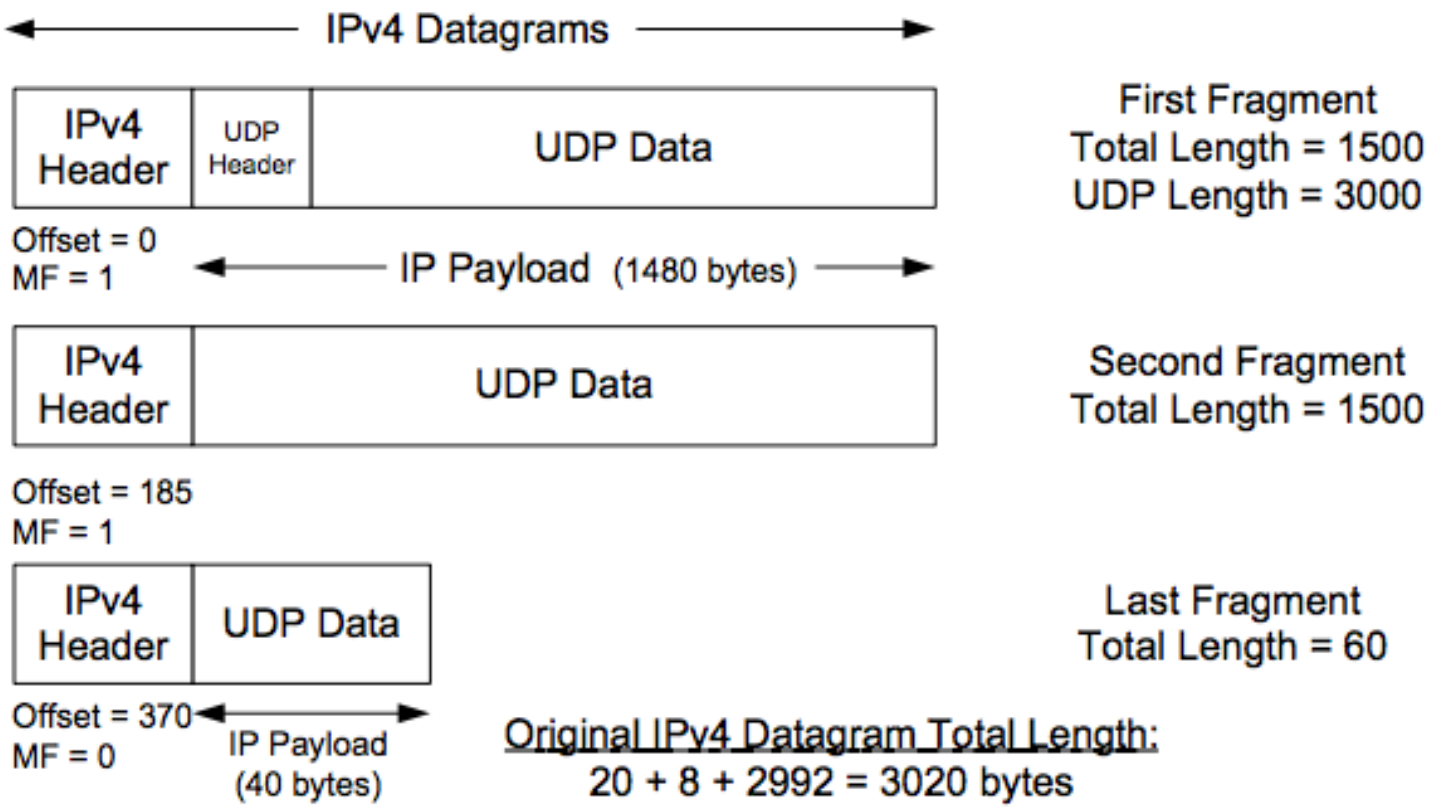
Tipos de Ataque DDoS: Reflexão/Amplificação



Tipos de Ataque DDoS: Fator de Amplificação



Tipos de Ataque DDoS: Porta 0???

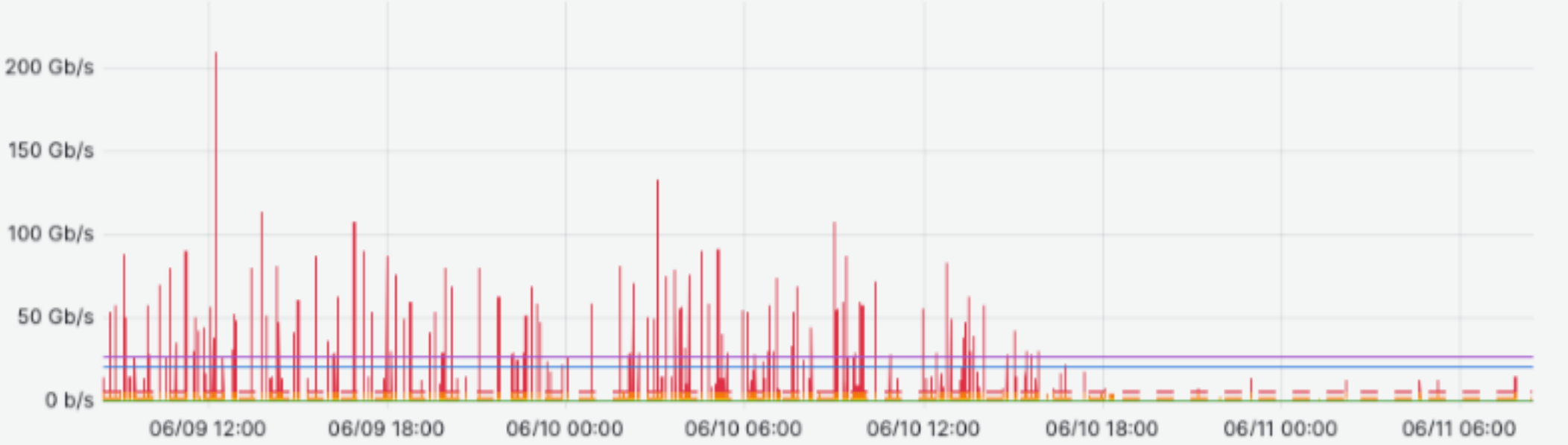


Tipos de Ataque DDoS: Hit&Run

- Imagine um moleque que aperta a campainha da sua casa e sai correndo
- Ataques de **curtíssima** duração <90s
- Mitigação complicada com as ferramentas tradicionais **baseadas em detecção**
- Criado por alguém que entende como funcionam as mitigações

OPENX

Tipos de Ataque DDoS: Hit&Run



Tipos de Ataque DDoS: Carpet Bomb

- Ataque em vários IPs simultaneamente (um /22 ou /24 por exemplo)
- 20Mbit x 1024 IPs > 20Gbit de tráfego

OPENX

O risco de não fazer nada!

O risco de não fazer nada!

- **Cancelamento** de clientes
- **Reclamações** nas Redes Sociais
- Danos à **reputação** do seu ISP
- **Sobrecarga/Perda de foco** no time técnico
- Entupimento atendimento (Whatsapp/ Telefone)
- **Perda de confiança**

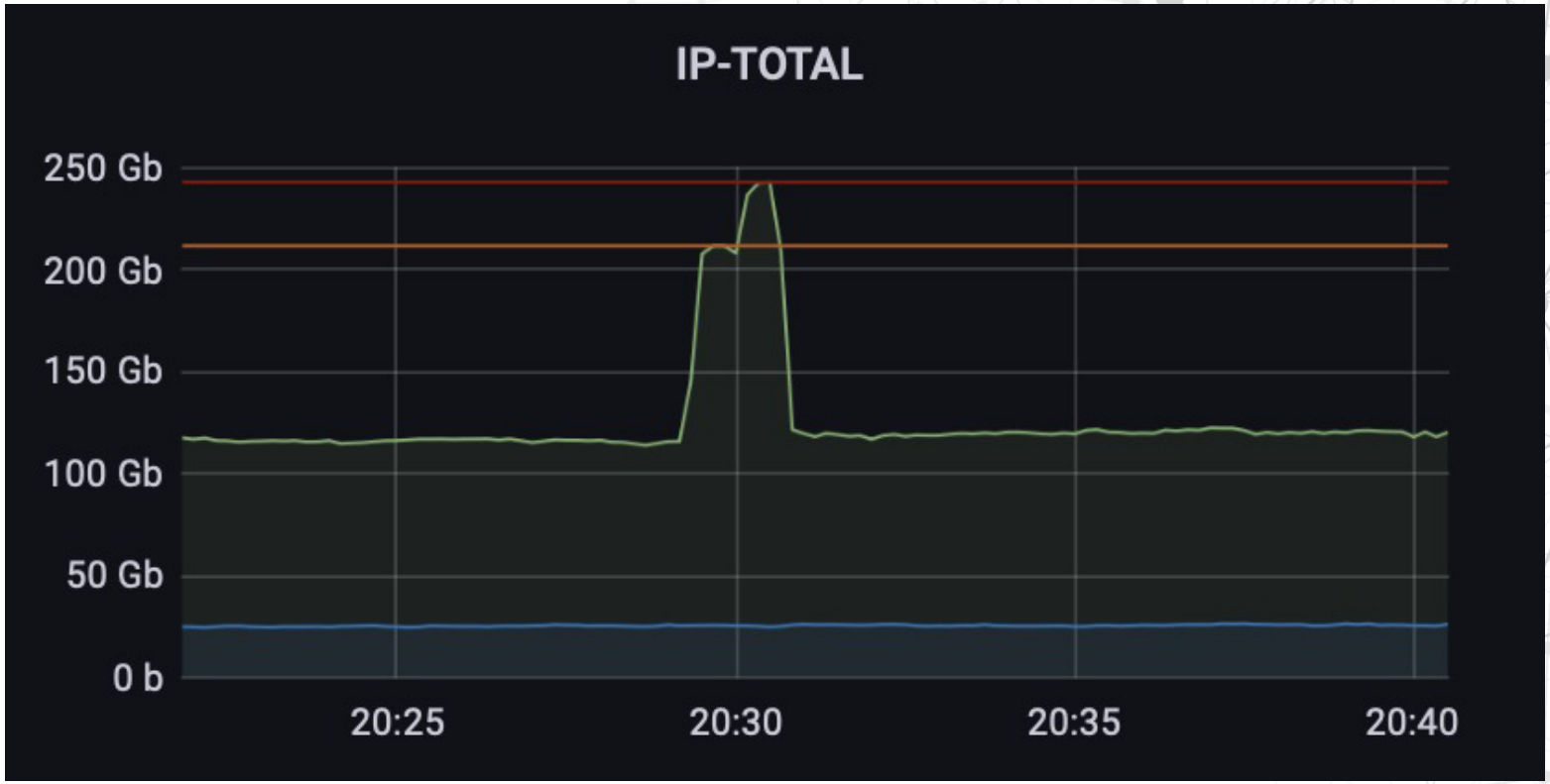
OPENX

Detecção de Ataque DDoS

É possível identificar um ataque DDoS através de:

- **Gráficos de consumo:** Sem detalhes, mas melhor que nada
- **Análise de flow (Netflow ou sflow):** Mais usado, muitas informações com um certo delay (30s a 60s)
- **Espelhamento de tráfego:** informação em tempo real, porém requer muita banda e processamento

Detecção de Ataque DDoS: Gráfico



Detecção de Ataque DDoS: Mirror

- Espelhar o tráfego para analisar em tempo real, todos os pacotes para identificar o ataque
- Requer muita banda e muito processamento mesmo em volumes "baixos" (10Gbit)
- Maquinas especiais conseguem analisar até 100+Gbit

Detecção de Ataque DDoS: Flow

- **Netflow (roteadores):**
  - Amostragem das sessões (conexões)
  - Muitos detalhes (ASN, nexthop e outras informações das rotas)
  - Maior Delay entre o evento e o flow
- **Sflow (switches e roteadores):**
  - Amostragem dos pacotes
  - Poucos detalhes (interface, cabeçalhos do pacote)
  - Menor Delay entre o evento e o flow
  - Traz os bytes iniciais do pacote

Detecção de Ataque DDoS: Flow

- **Fastnetmon:** Versão gratuita bem simples
- **Wanguard:** o melhor custo/benefício
- **Arbor:** Mais usado pelas operadoras (muito, muito caro)
- **Kentik:** Possui analises e dashboards focados em analise de ataques
- **Team Cymru Nimbus:** Boa alternativa gratuita e na nuvem

Detecção de Ataque DDoS: Wanguard

№	Prefix	IP Group	Anomaly	Speed	Sensor Interface	From	Duration	IP Pkts/s
680037	187.		NTP bits/s > 50.0 M	4.7 G	OX-GERAL	2023-05-09 23:03:48	2m 15s	1.3 M
679975	191.		TCP pkts/s > 100.0 k	5.2 M	OX-GERAL	2023-05-09 19:54:50	31m 31s	5.2 M
679941	102.		UDP-QUIC pkts/s > 1...	11.5 M	OX-GERAL	2023-05-09 15:00:29	9m 35s	11.5 M
679940	102.		DNS bits/s > 50.0 M	6.7 G	OX-GERAL	2023-05-09 15:00:29	4m 35s	1.7 M
679939	102.		INVALID bits/s > 50.0 M	11.1 G	OX-GERAL	2023-05-09 15:00:29	4m 35s	1.7 M
679842	191.		FIVE-M bits/s > 25.0 M	9.4 G	OX-GERAL	2023-05-08 23:55:46	2m	2.2 M
679731	191.		UDP pkts/s > 50.0 k	3.8 M	OX-GERAL	2023-05-08 09:16:36	3m 55s	3.8 M
679610	177.		DNS bits/s > 50.0 M	4.8 G	OX-GERAL	2023-05-07 18:29:18	58m 10s	1.2 M
679609	177.		INVALID bits/s > 50.0 M	7.7 G	OX-GERAL	2023-05-07 18:28:13	59m 55s	1.2 M
679600	177.		DNS bits/s > 50.0 M	5.5 G	OX-GERAL	2023-05-07 18:15:38	4m 55s	1.4 M
679599	177.		INVALID bits/s > 50.0 M	9.3 G	OX-GERAL	2023-05-07 18:15:38	4m 55s	1.4 M
679580	191.		FIVE-M bits/s > 25.0 M	9.0 G	OX-GERAL	2023-05-07 15:41:57	5m 55s	2.2 M
679567	191.		FIVE-M bits/s > 25.0 M	4.5 G	OX-GERAL	2023-05-07 14:57:36	7m 36s	1.2 M
679557	191.		FIVE-M bits/s > 25.0 M	7.1 G	OX-GERAL	2023-05-07 14:28:16	23m 35s	1.8 M
679550	191.		FIVE-M bits/s > 25.0 M	6.0 G	OX-GERAL	2023-05-07 14:08:16	7m 15s	1.5 M

Page 1 of 50 | 100 records per page | Displaying 1 - 100 of 4921

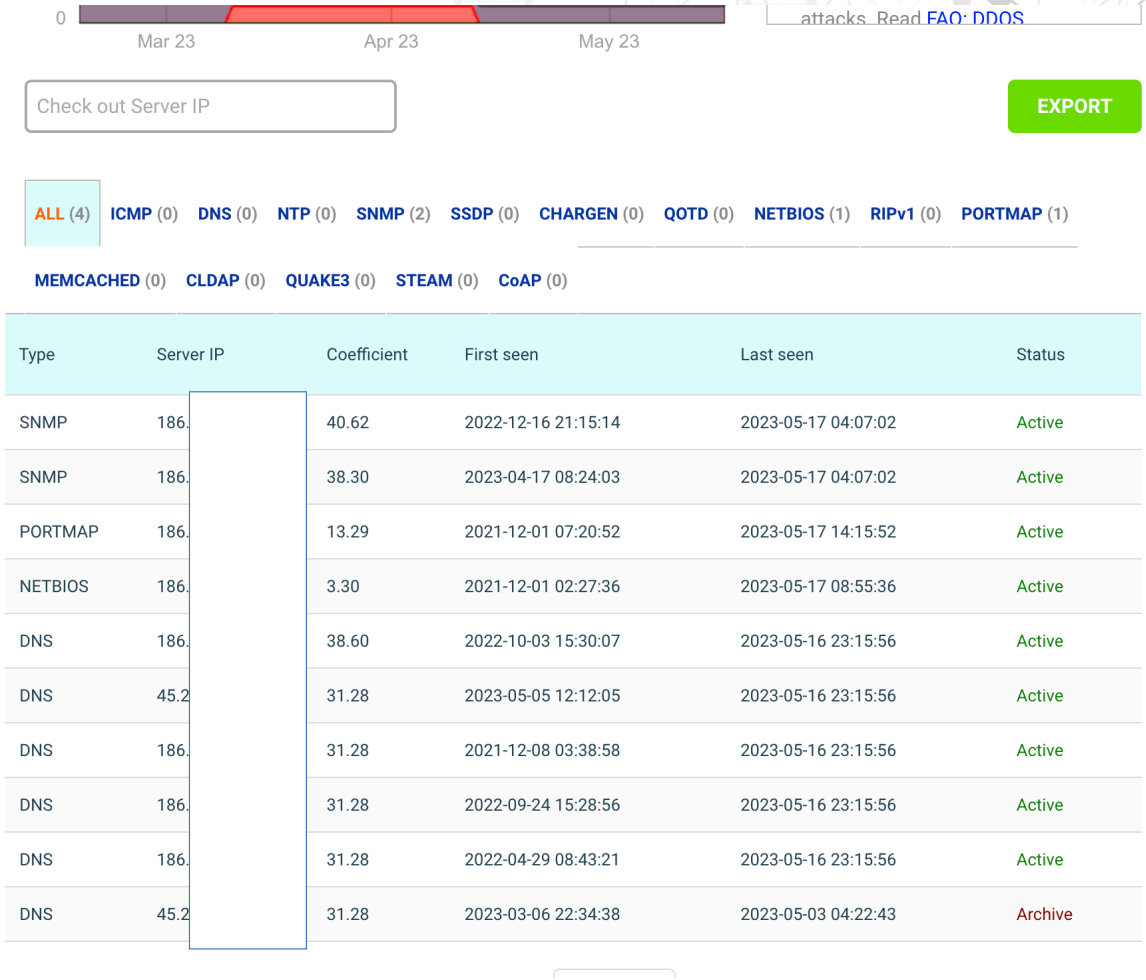
Prevenção de Ataque DDoS

As ações de prevenção não impedem que seu provedor seja alvo, mas vão ajudar com que a sua rede não seja origem ou amplificadora de ataques DDoS.

- **Anti-spoof/URPF:** Um roteador não pode aceitar pacotes com IPs de origem forjados
- **Configuração correta:** serviços que podem ser explorados para amplificação, principalmente **DNS, NTP, SNMP**
- **Filtro de portas:** clientes residenciais

OPENX

Prevenção de Ataque DDoS: Radar Qrator



Type	Server IP	Coefficient	First seen	Last seen	Status
SNMP	186.	40.62	2022-12-16 21:15:14	2023-05-17 04:07:02	Active
SNMP	186.	38.30	2023-04-17 08:24:03	2023-05-17 04:07:02	Active
PORTMAP	186.	13.29	2021-12-01 07:20:52	2023-05-17 14:15:52	Active
NETBIOS	186.	3.30	2021-12-01 02:27:36	2023-05-17 08:55:36	Active
DNS	186.	38.60	2022-10-03 15:30:07	2023-05-16 23:15:56	Active
DNS	45.2	31.28	2023-05-05 12:12:05	2023-05-16 23:15:56	Active
DNS	186.	31.28	2021-12-08 03:38:58	2023-05-16 23:15:56	Active
DNS	186.	31.28	2022-09-24 15:28:56	2023-05-16 23:15:56	Active
DNS	186.	31.28	2022-04-29 08:43:21	2023-05-16 23:15:56	Active
DNS	45.2	31.28	2023-03-06 22:34:38	2023-05-03 04:22:43	Archive

OPENX

Configurações de Firewall clientes residenciais

- Portas < 1024 (DNS, NTP, Email, SNMP)
- Porta 10001 (gerencia ubnt)
- Porta 11211 (memcached)
- Porta da gerencia das CPEs (depende do ISP)
- Porta 1900 (SSDP)

Monitoramento Contínuo

- Somente um monitoramento continuo vai permitir alertar e **agir rapidamente**.
- Isso vai evitar que você descubra **somente depois** que os clientes estiverem **reclamando**.

OPENX

Teste de Vulnerabilidades

- Fique sempre atento a correções de vulnerabilidades nos seus equipamentos e principalmente no que você instala dentro da casa dos clientes.
- Uma simples vulnerabilidade pode se transformar em milhares de zumbis prontos para atacar a partir da sua rede
- Teste se seus equipamentos (principalmente CPEs) estão vulneráveis

OPENX

Construindo uma Defesa com Aliados

- Quanto de link sobrando você tem? (burstable)
- É necessário muito link sobrando para suportar as variações de consumo sem impactar o dia a dia da sua operação em caso de ataques
- Sem isso, você precisa do apoio de alguma operadora que ofereça serviços de mitigação ou link IP já mitigado

OPENX

Identificando os Inimigos

- **Chantagem/extorsão:** O atacante entra em contato solicitando pagamento (bitcoin ou PIX) para cessar o ataque
- **Concorrência:** O mandante do ataque é uma empresa concorrente
- **Juventude:** Público Gamer
- **Retaliação:** Ataques à partir da sua rede te transformam em um alvo
- **Guerra:** atualmente as guerras também se desenvolvem no campo virtual (Russia x Ucrânia e Israel x Gaza)

OPENX

Como enfrentar um Ataque

- Tenha um bom **plano de ação**
- Tenha **ferramentas de detecção**
- **Possua link** com alguma operadora capaz de mitigar ataques DDoS
- **Colete** o maior número de informações
- **Denuncie**. A polícia brasileira tem sucesso em pegar os criminosos
- **NUNCA, NUNCA MESMO**, pague o criminoso em casos de extorsão

OPENX

Comunicação Durante o Ataque

- **Transparência** é fundamental
- Não permite que as **más noticias** sejam dadas por terceiros
- Principalmente **clientes ISP**, pois mesmo que os seus prefixos sejam protegidos, um ataque para um cliente ISP pode afetar a sua operação

OPENX

Mitigações Ataque DDoS

Dicionário

Definições de Oxford Languages · Saiba mais

mitigar

verbo

transitivo direto e pronominal

tornar(-se) mais brando, mais suave, menos intenso (ger. dor, sofrimento etc.); aliviar, suavizar, aplacar.

"m. a saudade, a sede, a ira etc."

Semelhantes

abrandar | acalmar | amansar | amortecer | aplacar | atenuar | conter

Mitigações Ataque DDoS

Técnicas para mitigar os efeitos de um ataque em andamento.

- Blackhole (RTBH)
- Scrubbing Center (Limpeza de tráfego)
- BGP-Flowspec
- **OpenX ActiveGuard**

Mitigações Ataque DDoS: Blackhole (RTBH)

- Através de uma community BGP um IP (/32) é marcado para descarte do tráfego na rede da operadora ou IX.br
- Muito pouco eficaz atualmente

Mitigações Ataque DDoS: Scrubbing Center

- O tráfego é redirecionado para um dispositivo que analisa o ataque identificando o padrão do ataque e descartando o tráfego sujo.
- Se for muito "rígido", pode gerar falso positivo, descartando tráfego legítimo.
- Se for muito "flexível", pode gerar falso negativo, deixando tráfego malicioso passar.
- Quanto mais próximo do provedor, melhor, pois não aumenta a latência e não prejudica o dia-a-dia.
- Evitar túneis pois podem degradar a performance.

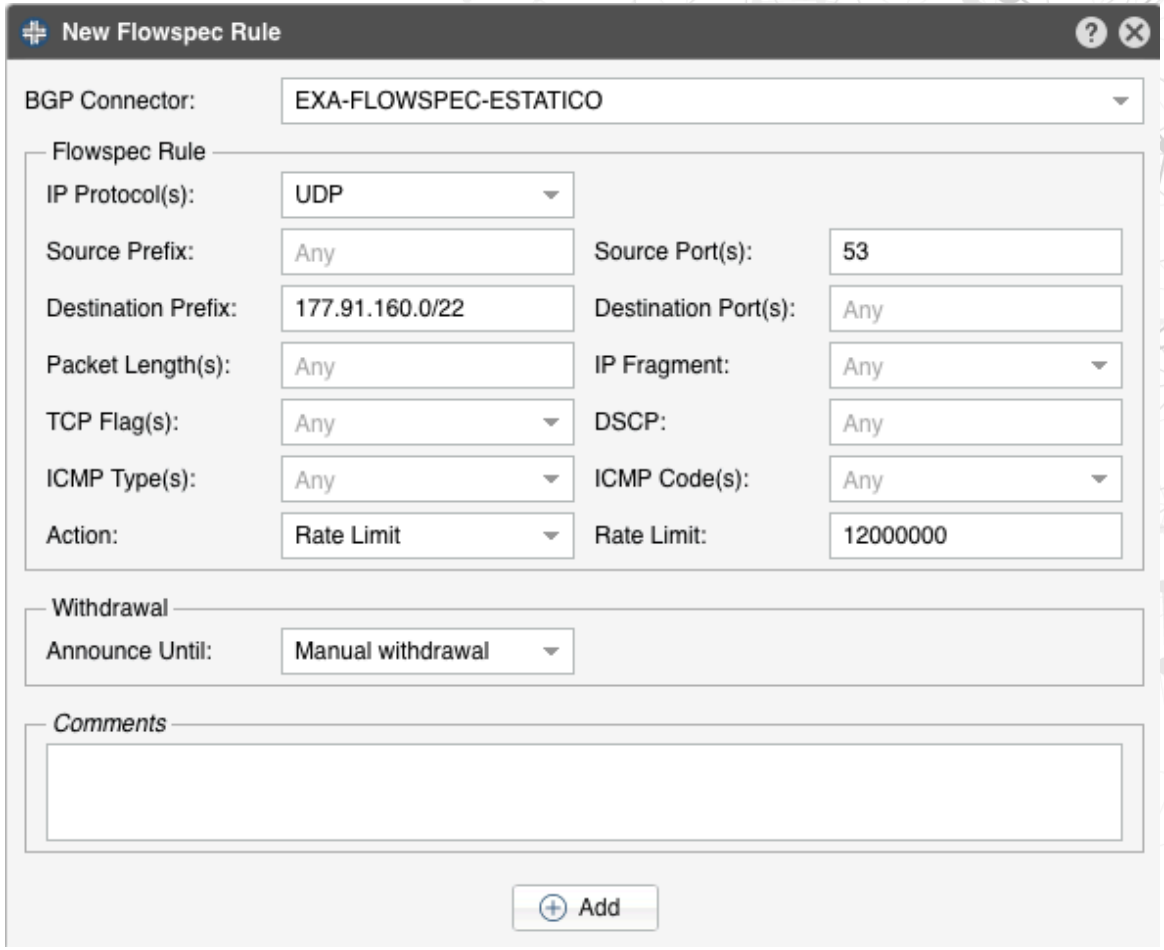
OPENX

Mitigações Ataque DDoS: FlowSpec

- Mecanismo que usa BGP para propagar regras de firewall que serão aplicadas na rede da operadora, evitando que o tráfego ilegítimo chegue ate o provedor.
- Poucas operadoras suportam esse recurso.
- Precisa de uma ferramenta para gerar as regras (script+exabgp ou Wanguard, por exemplo)
- A ação de uma regra pode ser aceitar, limitar ou rejeitar o tráfego

OPENX

Mitigações Ataque DDoS: FlowSpec



Mitigações Ataque DDoS: OpenX ActiveGuard

- Com o surgimento dos ataques Hit&Run, percebemos que precisávamos ajudar nossos clientes para que o **impacto** dos ataques fosse **reduzido** usando algo que ficasse sempre ativo.
- Surgiu a ideia de fazermos um filtro que ficaria **ativo** o tempo todo derrubando o tráfego ilegítimo e limitando o tráfego de aplicações legítimas, mas que são usadas como vetor de ataques DDoS (por exemplo DNS e NTP)
- Em Janeiro de 2023, percebemos que essa tecnologia **OpenX** absorveu um ataque de 150Gbit na sua totalidade.

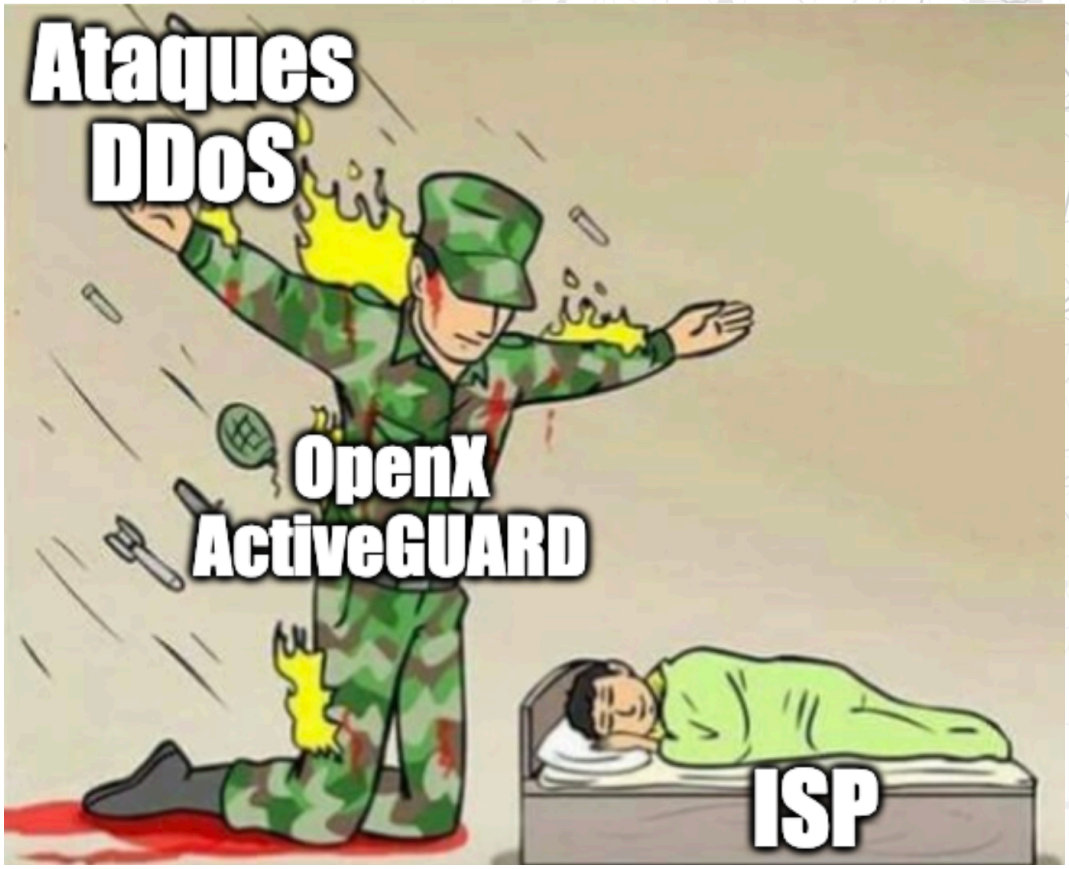
OPENX

Mitigações Ataque DDoS: OpenX ActiveGuard

- Esse desempenho nos mostrou que esta ferramenta possuía um **enorme potencial**
- Resolvemos então **desenvolver** e **evoluir** as regras de proteção, usando nosso **conhecimento** em ciber segurança e analise de dados

OPENX

Mitigações Ataque DDoS: OpenX ActiveGuard



OpenX ActiveGuard: Principais características

- Não depende de **detecção** para mitigar o ataque
- O dia-a-dia tem que **funcionar sempre**
- Filtra 99% das ameaças **automaticamente**
- Capacidade de mitigação é a **mesma capacidade total** do nosso backbone
- Não usa túneis e nem envia o tráfego pra fora da nossa rede
- **Dashboards** para o acompanhamento do ataque
- Link IP de **altíssima qualidade**

OPENX

Análise *Post-Mortem*

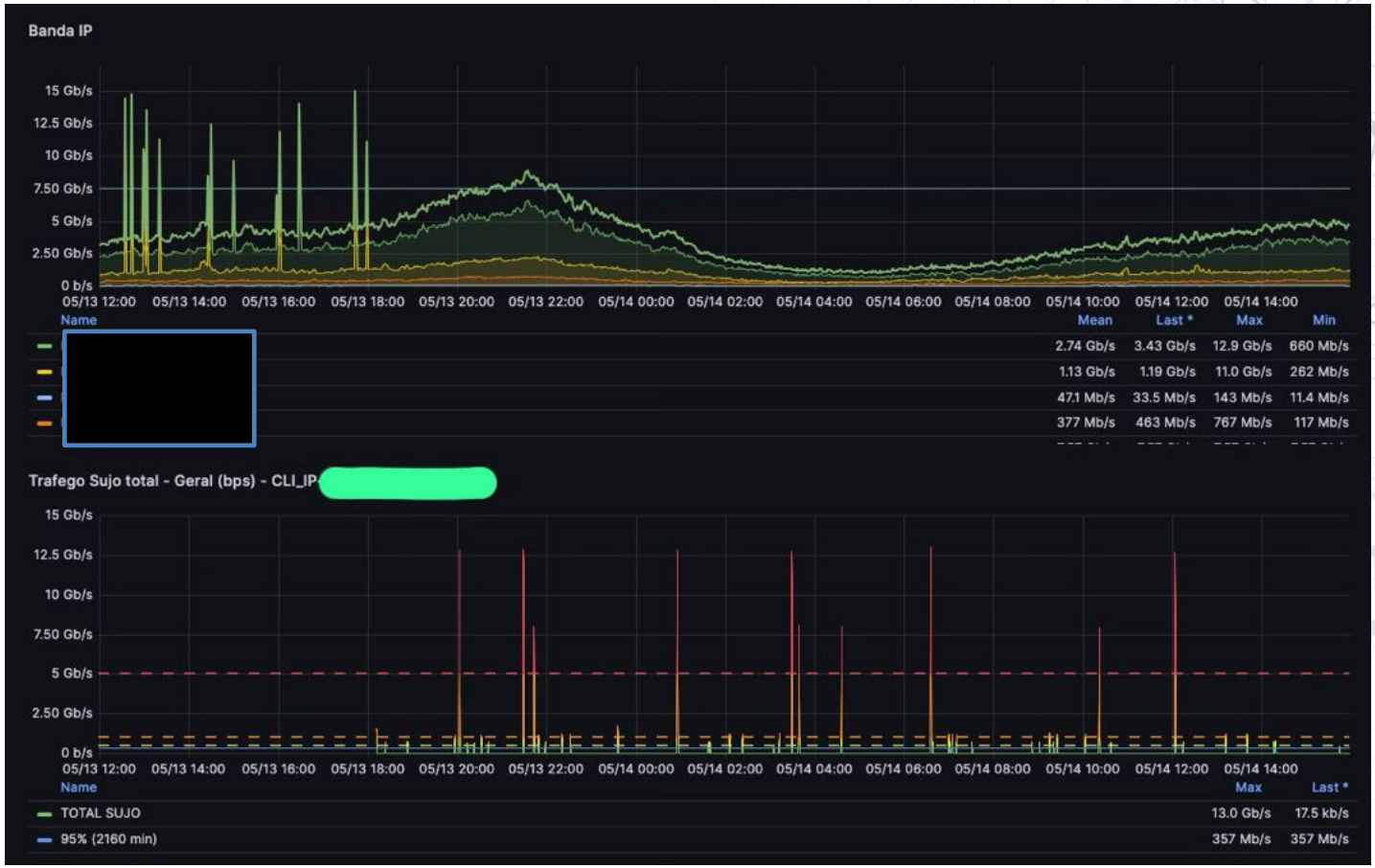
- Passo extremamente importante.
- Avaliação do ataque e seus danos.
- Aprendizado para futuras defesas.
- **Time OpenX é o responsável por isso sempre executa essa etapa!**

Benefícios de uma Defesa Eficiente

- **Tranquilidade** para focar no seu negócio
- **Diminuição** das reclamações
- **Redução** nos cancelamentos
- **Melhor experiência** do usuário, sem interrupções

OPENX

Histórias de Sucesso



Implementação de Melhorias

- Na OpenX, sempre que algum **ataque novo** surge, adaptamos as **nossas defesas** (vacina) em todos os roteadores.
- Também melhoramos sempre a nossa parte de **monitoramento**, inclusive no painel dos clientes para que eles tenham uma melhor **visibilidade** sobre os ataques que foram **neutralizados**.

OPENX

Treinamento Contínuo

- Nosso time é **constantemente** treinado em **analise** das métricas e fluxos de dados para **desenvolver** novas "vacinas" para os **novos ataques** que surgem.

OPENX

Novas Ameaças e Desafios

- Cada **nova ameaça** detectada é testada primeiro em um cliente, confirmamos se esta **funcionando** dentro do esperado (sem falsos positivos e negativos) e depois replicada para todos os outros clientes

OPENX

Preparando-se para o Futuro

- A **OpenX** tem um extenso planejamento de melhorias tanto no filtro quanto no monitoramento em tempo real.
- **Novos POPs** pelo Brasil: BH, POA, CTB, RJ, BSB, SSA, além de Fortaleza e SP

OPENX

Conclusão

- **Detecção**: Ser capaz de dizer se sua rede esta sob ataque
- **Prevenção**: Ações para impedir que a minha rede seja usada para atacar outras empresas
- **Mitigação**: Técnicas que vão minimizar o impacto de um ataque DDoS

OPENX

Perguntas?


Inovação é resolver um problema de um jeito que ele ainda não foi resolvido!

Obrigado!

YouTube.com/openx
Instagram: @openxbr e @renatoornelas
LinkedIn.com/company/open-x/

OPENX